



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/582,206	07/17/2000	ALEXANDER ANDRAAVICH MOLDOVYAN	P65724USO	4821

7590 06/03/2004

JACOBSON, PRICE, HOLMAN & STERN
400 SEVENTH STREET N W
SUITE 600
WASHINGTON, DC 20005

EXAMINER

SEAL, JAMES

ART UNIT PAPER NUMBER

2135

DATE MAILED: 06/03/2004

8

Please find below and/or attached an Office communication concerning this application or proceeding.

fr

Office Action Summary

Application No.

09/582,206

Applicant(s)

MOLDOVYAN ET AL. 

Examiner

James Seal

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 18 March 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-3 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-3 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☒ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

Art Unit: 2135

DETAILED ACTION

1. This Action is in reply to applicant correspondence dated 18 March 2004.
2. Substitute specification has been entered.
3. Amended claims 2 and 3 have been entered.
4. Claims 1-3 are pending

Specification

5. With the substitute specification, objection withdrawn.

Oath/Declaration

6. Examiner notes page 5 of response that applicant is preparing for filing a substitute declaration.

Claim Objections

7. Claim 1 objected to because of the following informalities: In claim 1, line 2, the word *alternate* should be *alternately*. Objection maintained. Appropriate correction is required.

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

9. Claims 1-2 are rejected under 35 U.S.C. 102(b) as being anticipated by

Art Unit: 2135

Delayaye et. al. US 4751733 A.

10. As per claim 1, the limitation of a method for cryptographic conversion (Encryption) of binary data blocks disclosed by Delayaye see Column 1, 8-10, consisting of slitting the data blocks (words consisting of n bits) into two or more ($N \geq 2$) sub-blocks (sub-words of m bits) see Column 1, line 13-14 and Figure 3 (note in this case Delayaye splits the word element 9 into four 32 bit words and places them in the latches, Converting said blocks by performing an encryption of the i th sub-block such (see figure 1 elements 2, 3, 4, 5 the encryption being carried out by parts of the word to be encrypted and by parts of the key, Column 8, 45-47) and thus these parts would be latched into 20 and 21 Figure 3. Thus in this mode of operation, part of sub-block can be used in the encryption of sub-blocks 13 and 14. Thus the operation of transposing (encrypting) bits of the i th sub-block is used as the operation dependent on the value of the j th sub-block. Claim 1 is rejected.

11. As per claim 2, that the limitation of transposing bits as disclosed in 1 is further characterized in that the transposition is generated and dependent on a secret key before the beginning of the i th sub-block conversion (encryption). Referring to Figure 1 of Delayaye, keys are stored in the key memory element 7 and are distributed to the substitution boxes before the encryption of the sub-blocks occur, see Column 2, lines 66-68, Column 3 lines 1-16. Claim 2 is rejected.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

Art Unit: 2135

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Delayeye as applied to claims 1-2 above, and further in view of Mittenthal, Statistically Efficient Inter-Round Mixing Block Substitution Devices January 1996.

12. As per claim 3, the limitation of the transposition of the i th row depends on that of the j th row and further characterized that a binary vector V is additionally generated, said operation of transposing bits of said i th sub-block being performed depending on the V value, where the binary vector is generated depending on its value at the time of performing the preceding step of converting one said sub-blocks and depending on the j th sub-block, is disclosed by Mittenthal page 3 bottom. Note feed forward loops from the i to the $i+1$ S-box. One of ordinary skill in the art at the time of the invention would have been motivated to have modified Delayeye invention with the teaching of Mittenthal to have given a better statistical distribution for the substitutions (permutations), and because this increases the resistance to attack from differential and linear attacks. Claim 3 is rejected.

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the

Art Unit: 2135

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Response to Arguments

13. Applicant's arguments filed 18 March 2004 have been fully considered but they are not persuasive.

14. Applicant does not claim "two-place operations, fixed bit transposition, and controlled bit transposition". Although the claims are interpreted in light of the specification, limitation from the specification are not read into the claims. In re Van Guens, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993)

15. Further Delayaye discloses "numerous variations which could be made to the device thus described without departing from the spirit of the present invention" Column 8, lines 17-20, and then goes on to mention "changing the orders of the operation (permutation-substitution PS instead of substitution-permutation SP)" so that permutations (or substitution) might occur in succession SPPS (See Delayaye Column 8, lines 24-29). However, the permutation on n objects form a group and so the product of two permutation is another permutation (closure). Thus applying two permutation is equivalent to applying only one permutation and thus it would not be a variation of the original case. The only way to make two successive permutations give a variation of the original invention "without departing from the spirit of the invention" is for the second (or first) permutation to change with each bit.

Art Unit: 2135

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to James Seal whose telephone number is 703 308 4562.

The examiner can normally be reached on M-F, 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703 305 4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

JWS

Jws
AU 2135
30 May 2004



KIM VU
ELECTRONIC BUSINESS CENTER 2135